Real World Desktop Management Practices

Session 644

These are confidential sessions—please refrain from filming or taking pictures.

Enterprise IT

Real World Desktop Management Practices

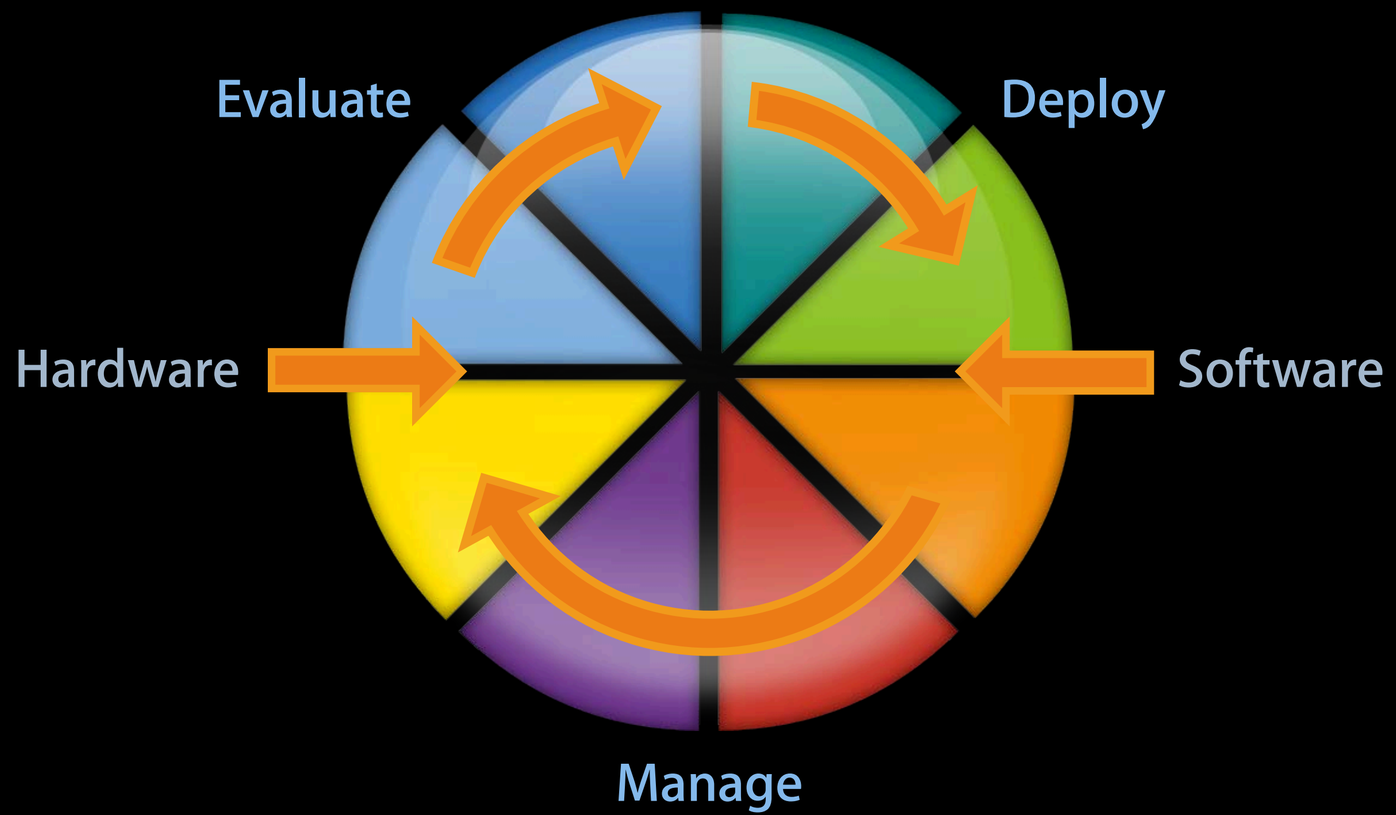
http://developer.apple.com/wwdc2005/

Agenda

- Introduction
- Systems Lifecycle and tasks
- Open Source and the lifecycle
- Q&A

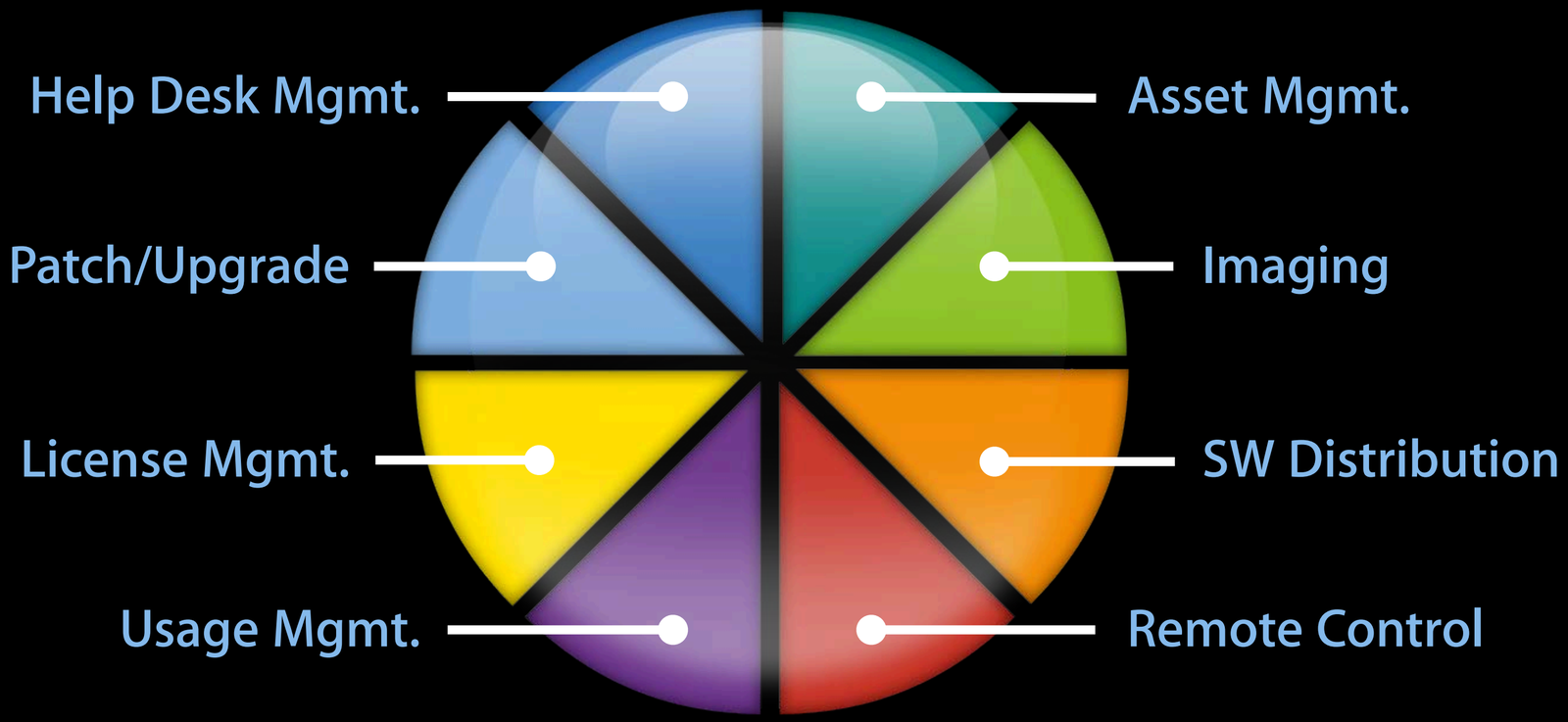
Systems Lifecycle—What Is it?

- Task oriented process of systems management
- Cyclical—usually involves a yearly rotation
- Focuses on three stages:
  - Evaluate
  - Deploy
  - Manage



Lifecycle Tasks

The bread and butter of IT



Evaluation

Determining the best infrastructure mix

- Which tasks must I do in-house/outsource?
- What software/hardware is needed?
- How much manpower do I need?
- How often am I going to perform <task>?
- How do I get a raise?

Deployment

Turning common systems into unique systems

- How many system images do I need to build/maintain?
- How many systems must I deploy at once each cycle?
- How much of my deployment is
  - Manual?
  - Network-based?
  - Seat of the pants?
- How long does it take to deploy my systems?
  - Full refresh
  - Partial refresh
  - Iterative/repair
- How often do I refresh my systems?

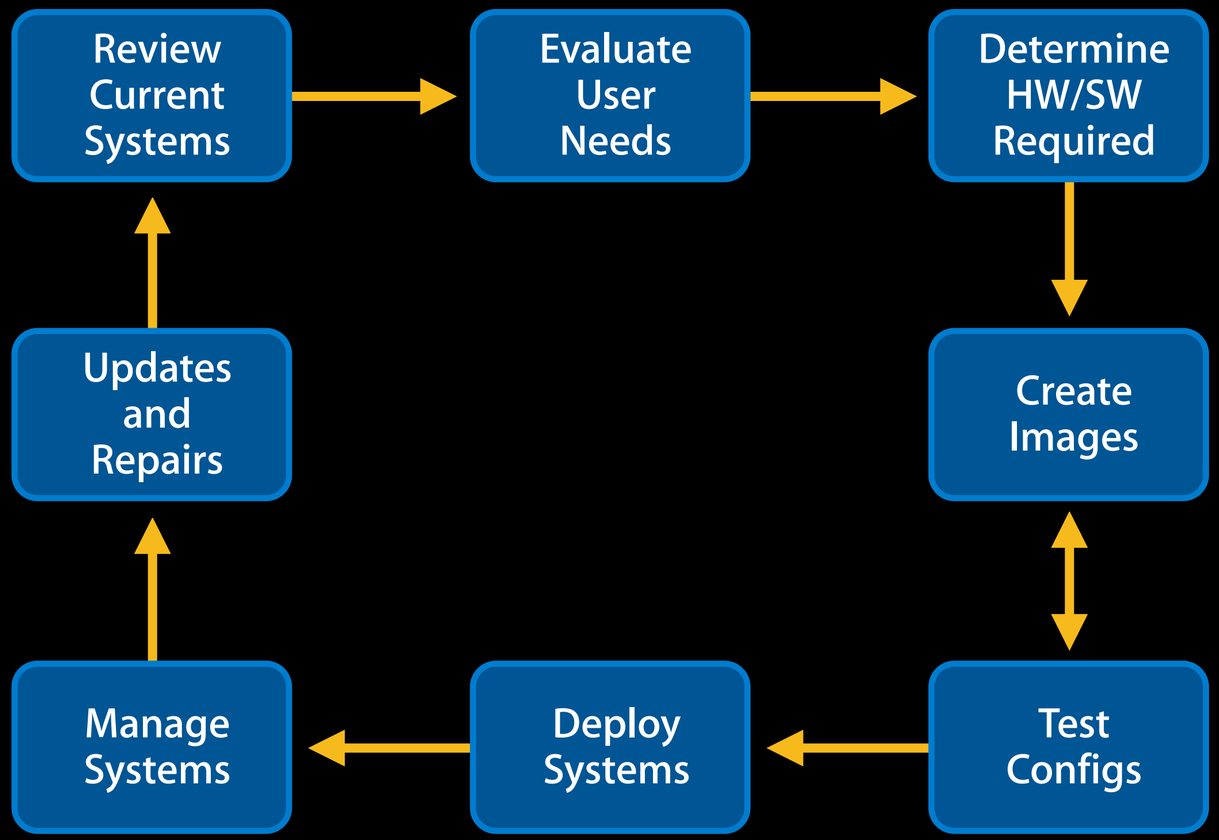
Management

Maintain and support the environment

- Is systems management going to be centralized?
- What about license management?
- Who handles simple password changes?
- System software and security updates?
- Hardware replacement—user/client data?
- Third party application updates?
- Who handles help desk operations?
- What about client/workflow management?
- What about asset management?
- Where's that pay raise?

Lifecycle in Action

Yearly Refresh Example



Task Examples

Defining the tasks with Apple-based solutions

- Asset Management/Remote Control/Help Desk Ops
  - Apple Remote Desktop
- Imaging systems
  - NetInstall/ASR-multicast
- Software Distribution
  - ARD/NetInstall
- Usage Management
  - Workgroup Manager/MCX
- Patching and Upgrading
  - ARD/NetInstall

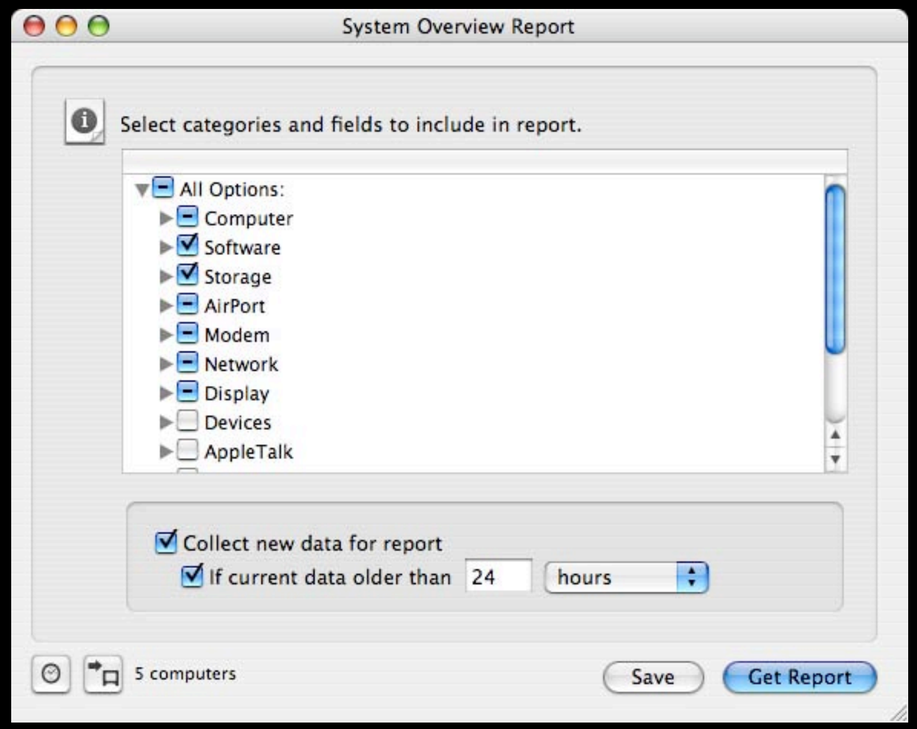
Picking Solution Sets to Meet the Tasks

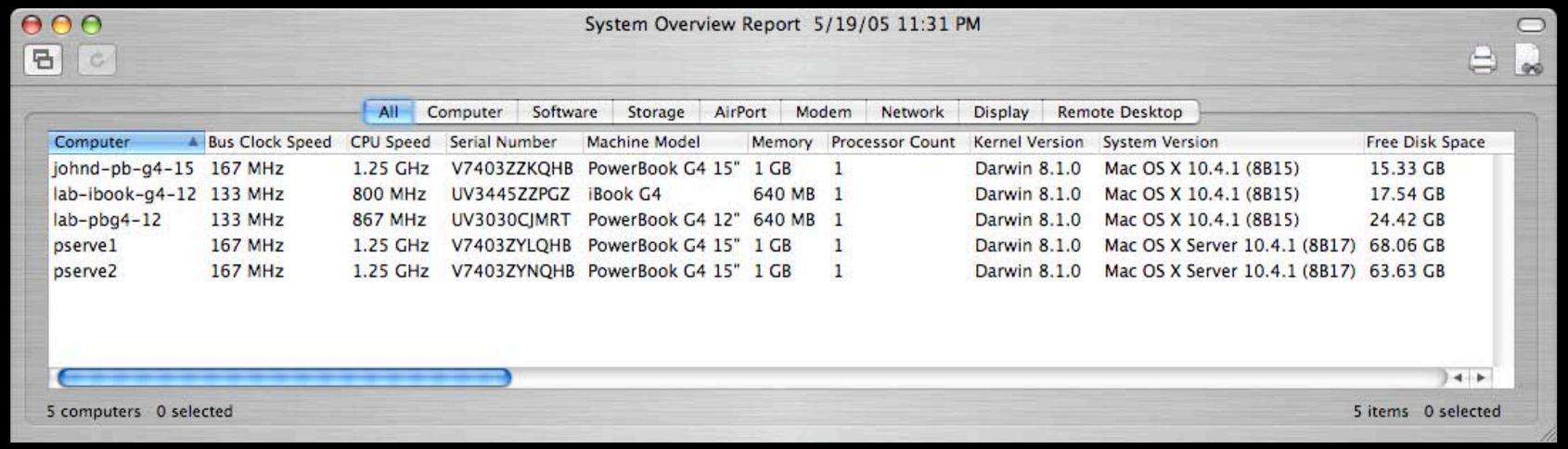
- Unified tool set versus ‘Best of breed’
- Cost of Ownership versus IT expertise
- Task versus Tool
  - Imaging <> NetInstall/NetRestore
  - Updating <> ARD/radmind
  - Managing <> MCX/ARD
- Focus on the result—not the tool/task
  - “Are my users able to accomplish their jobs?”
- Remember the 90/10 rule…

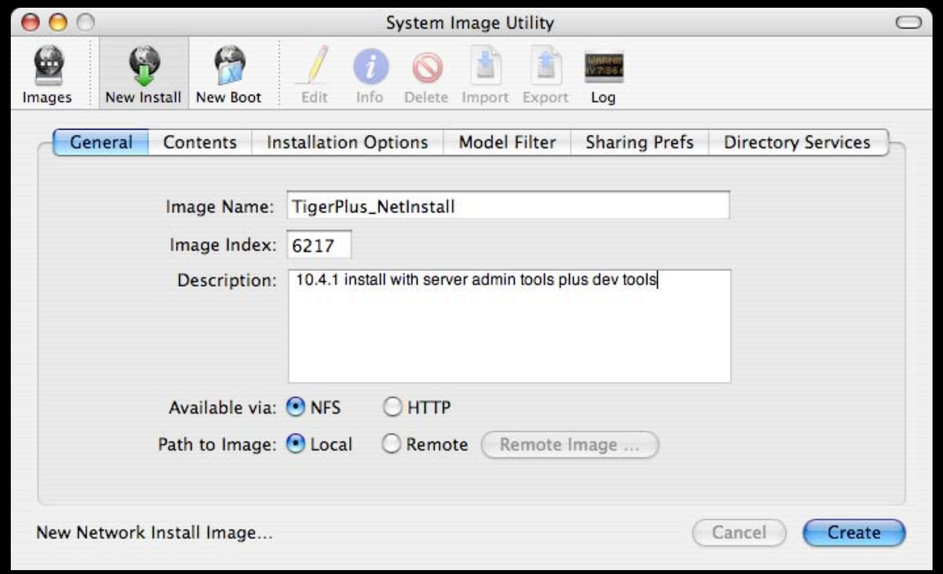
Asset Management

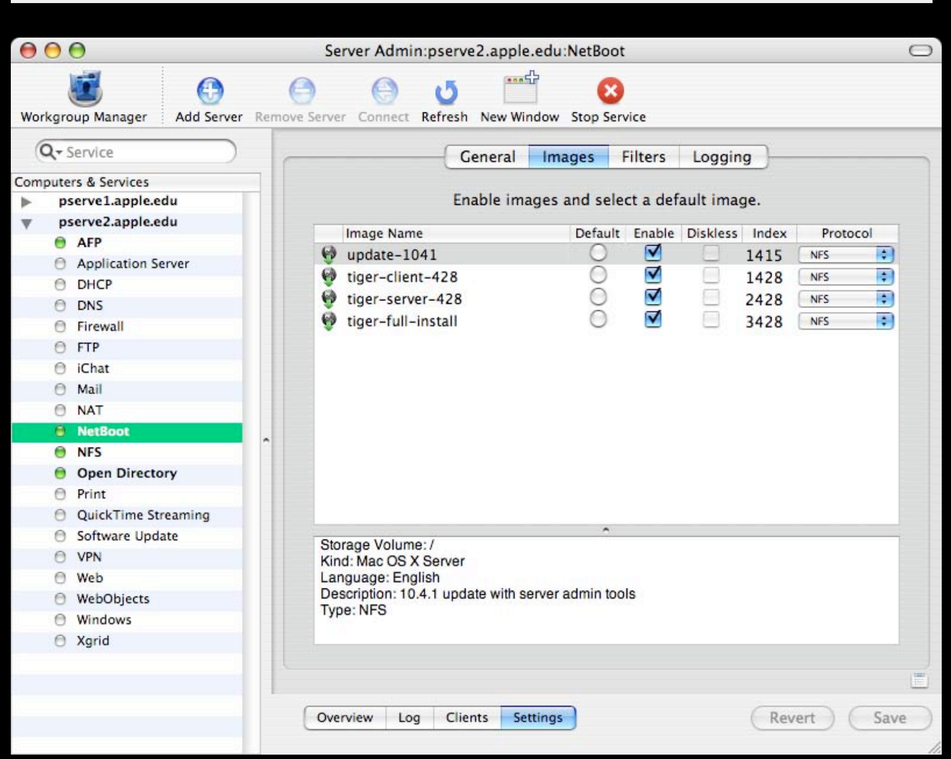
Apple Remote Desktop

- System reports
- Network reports
- Memory reports
- Device reports
- File search









Imaging Systems

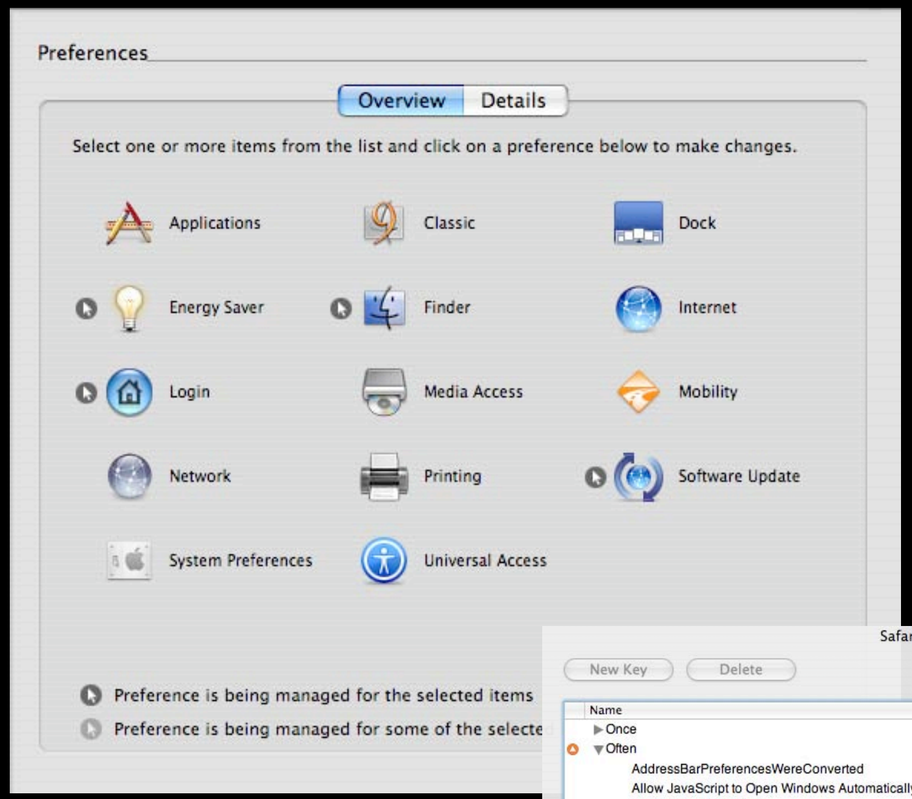
NetInstall

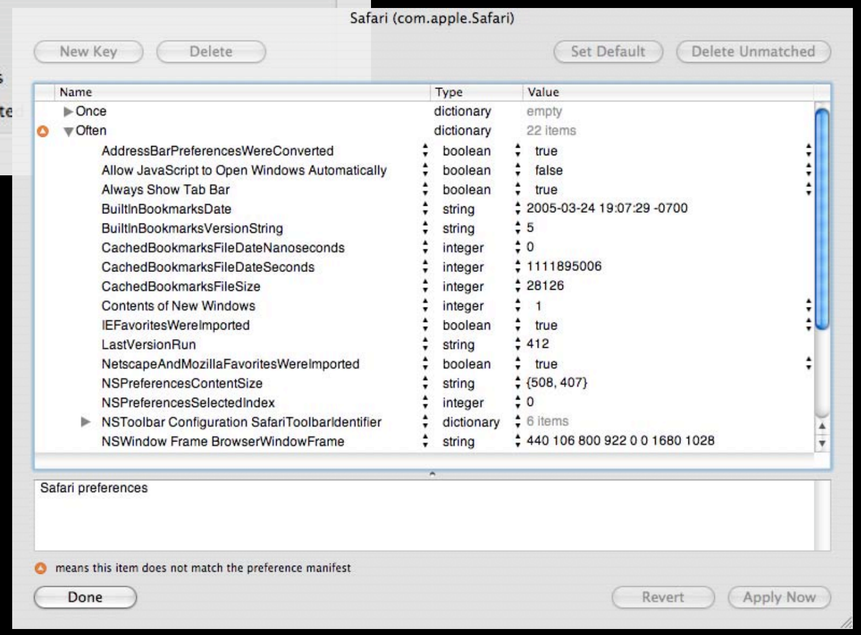
- Core OS installs
- Customized OS-plus installs
- Application only installs
- Upgrade installs

Usage Management

Managed Client for OS X

- Granular control of system preferences at user/group or computer level
- Third party preference editor
- Mobile account and portable home directory support





Open Source Tools for Lifecycle Tasks

Customer usage scenarios

http://developer.apple.com/wwdc2005/

Steven Doyle

Edith Cowan University,
Perth, Western Australia
Faculty of Communications and Creative Industries

http://developer.apple.com/wwdc2005/

About CCI

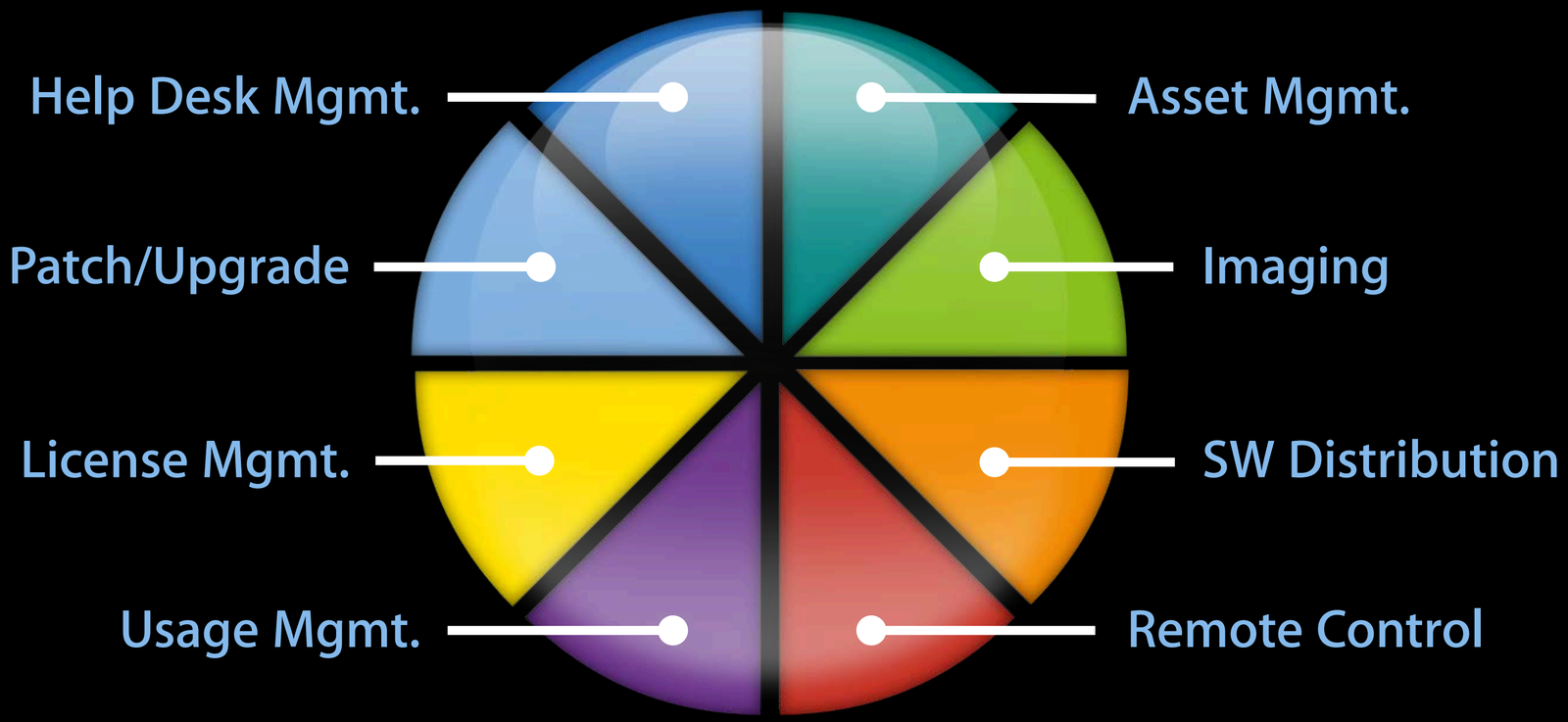
- School of Communications and Multimedia
- Largest in Australia, over 500 students
  do a common foundation year as a first year
- Disparate streams offered
- Supporting minors from SOCA or compSci

Streams

Advertising	PR	Textile	Lighting Design
MultiMedia	Digital Media	Print Graphics	Radio Broadcast
Film & Video	Hat Making	Packaging Design	Television Broadcast
Journalism	Pro Audio	Set Design	Final Cut Editing
Mass Comms	Pro Tools	CAD	Digital PhotoMedia
Media Studies	Logic	Costume Design	
PhotoMedia	Midi	Musical Scoring	

Lifecycle Tasks

The bread and butter of IT



Machines

- How to image them
- How to maintain them imaged
- How to monitor them
- How to asset track them
- How to track their usage

User Management

- Transient student population
- 24/7 isn’t enough
- License challenges
- Powerbooks
- Peecee’s

Separate Yet Connected Areas

- All IT management related
  - Lab isn’t a lab anymore
  - A workstation isn’t one person’s or in one place!
- If it’s a computer it ends up with us
- Impossible to manage/control/forecast/plan

Help Desk System

- We wrote a help desk
- Open sourced
- php/mysql/shell
- Leverages heavily on ARD 2

Why?

- Didn’t like any of the off-the-shelf ones
  - Why?
  - Their shelf is expensive
  - Didn’t meet our needs
  - Scalability issues

Why?

- We were constantly entering the same data
  - Purchasing system
  - Login system
  - Management system
  - But still losing track of information
  - Machines would go “missing”
  - New machines would magically appear

Feature Summary

- MySQL
- PHP
- Needs documentation
- Module-based
- Scaleable
- Designed for low-end users (aka helper monkeys)
- Today I’m just going to talk about the ARD stuff

Highlight Summary

- ARD Features
- Powerful hardware searches
- Lab Organization/Imaging Options
- WorkGroup Manager
- Machine on network status
- Imaging
- Packaging making

ARD 2

- Client/server model
- Comes with a data collection model
- Stores data in centralized server
- In a postgres database

PostgreSQL
phpPgAdmin
public
Tables
propertynamemap
systeminformation

ard: propertynamemap

Field	Type	Not Null	Default	Actions		Comment
objectname	character varying(128)	NOT NULL		Alter	Drop	
propertyname	character varying(128)	NOT NULL		Alter	Drop	
propertymapid	integer			Alter	Drop	

ard: systeminformation

Field	Type	Not Null	Default	Actions		Comment
computerid	character(17)	NOT NULL		Alter	Drop	
objectname	character varying(128)	NOT NULL		Alter	Drop	
propertyname	character varying(128)	NOT NULL		Alter	Drop	
itemseq	integer			Alter	Drop	
value	character varying(512)			Alter	Drop	
lastupdated	timestamp with time zone			Alter	Drop	

Mac_SystemInfoElement	WirelessCardIsActive	0
Mac_SystemInfoElement	WirelessCardFirmwareVersion	1
Mac_SystemInfoElement	WirelessCardHardwareAddress	2
Mac_SystemInfoElement	WirelessCardLocale	3
Mac_SystemInfoElement	WirelessCardType	4
Mac_SystemInfoElement	WirelessCardInstalled	5
Mac_SystemInfoElement	WirelessChannelNumber	6
Mac_SystemInfoElement	WirelessNetworkAvailable	7
Mac_SystemInfoElement	WirelessIsComputerToComputer	8
Mac_SystemInfoElement	WirelessNetworkName	9
Mac_SystemInfoElement	AppleTalkIsActive	10
Mac_SystemInfoElement	AppleTalkNetworkNumber	11
Mac_SystemInfoElement	AppleTalkNodeNumber	12
Mac_SystemInfoElement	AppleTalkZone	13
Mac_SystemInfoElement	ActiveProcessorCount	14
Mac_SystemInfoElement	UserMemorySize	15
Mac_SystemInfoElement	BootROMVersion	16
Mac_SystemInfoElement	BusSpeedString	17
Mac_SystemInfoElement	BusSpeed	18
Mac_SystemInfoElement	BusDataSize	19
Mac_SystemInfoElement	ProcessorSpeedString	20
Mac_SystemInfoElement	ProcessorSpeed	21
Mac_SystemInfoElement	MachineSerialNumber	22

computerid	objectname	propertyname	itemseq	value	lastupdated
00:0d:93:9b:ac:06	Mac_FireWireDeviceElement	DataDate	0	2004-08-23T02:07:53Z	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_FireWireDeviceElement	DeviceSpeed	0	400mbit_speed	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	DataDate	0	2004-08-23T02:07:53Z	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	CreationDate	0	2004-05-20T05:12:38Z	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	FileSystemType	0	18475	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	FreeSpace	0	75132600	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	GroupName	0	admin	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	IsBootVolume	0	true	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	IsCasePreserving	0	true	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	IsCaseSensitive	0	false	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	IsWritable	0	true	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	JournalingIsActive	0	true	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	LastBackupDate	0	2004-05-20T05:12:38Z	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	LastConsistencyCheckDate	0	2004-08-23T02:07:53Z	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	LastModificationDate	0	2004-08-23T02:07:53Z	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	OwnerName	0	root	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	PermissionModes	0	17405	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	PermissionsAreEnabled	0	true	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	RemovableMedia	0	false	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	SupportsJournaling	0	true	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	TotalFileCount	0	106759	2004-08-23 02:07:53+08
00:0d:93:9b:ac:06	Mac_HardDriveElement	TotalFolderCount	0	25249	2004-08-23 02:07:53+08

Help Desk Workflow Model

- Incredible leverage opportunities from ARD's thorough database capabilities
- Powerful integration options with our own mysql database
- Goal for one stop management console for admins and nominated admins
- I want it powerful for the powerful, but simple enough to delegate

Machines on CCI subnets

Machines in ARD Postgres Database

Machines in MySQL HelpDesk Database

Work Flow

- The data that we manipulate on a regular basis lives in local mysql database
- Regular scans of ARD database to update mysql (user defined)

Work Flow

Machines in MySQL HelpDesk Database

Machines in ARD Postgres Database

Web Sharing Status

Free RAM Slots

Drive Free Space

Wireless Status

SSH Status

System Version

SMB Sharing Status

Allocate Machines to Labs

- Lots of machines in system(s)
- We track machines based on their physical location if they are lab machines (paint your wall!)
- Or based on a group membership if not
  - So staff portables
- But new machines or moved machines cause us grief…
- So we use the help desk system to control all imaging/deployment
  The new version supports 10.4's multicasting too

Double Entry?

- We do a lot of work with WorkGroup Manager (WGM) to handle client management
- We do most of our stuff at the computer list level
- WGM prior to 10.4 has no facility for easily adding multiple computers
- The help desk system allows you to generate a text list suitable for importing directly into WGM

Machine Tracking

- Searches the ARD generated list (set ARD scheduled task for X minutes)
- Searches the mysql databases
- Looks for missing or extra ones…alerts the admin user

Machine Monitoring

- Running a large environment it's best to be proactive rather than reactive
- The system can be configured to "watch" for change states between scans on the machines, and then alert people of the change in states
- Why?
  - Projector disconnects
  - Student altering machine settings
  - Theft/damage
  - "This mouse has never worked"

Machine Status Monitoring

- Alerts are
  - iCal events for on task person
  - Logged jobs
  - Emails
  - (Or a combination)
  - Managers love it…staff not so much
  - [Yes it can do SMS as well but they begged me to not implement it]

Sample Alerts

- Drive Free Space (user specified range alteration)
- SSH Status (on/off)
- System Version (changed?)
- Free RAM Slots (changed or defined)
- Web sharing status (on/off)
- Windows sharing status (on/off)
- Wireless status (on/off)
- Mouse/Keyboard connection (on/off)

Package Maker

- One problem is that ARD allows for package pushing, but package making remains a task for the power users
- We needed away of delegating packaging making to sub-sys admins
- For example if we wanted to change the desktop pattern of a group of machines

Full Automation

Machine Delivered

Barcode scanned

Data entered into HelpDesk system

Destination selected

Machine Net Boots and installs Image

Logs its imaging time

Record user interactions

What I Didn’t Talk About

- Integrates into an asset management system
- HelpDesk system fully customisable

Who to Contact

Steven Doyle
ichat/email
stevendoyle@mac.com

James Reynolds

University of Utah

http://developer.apple.com/wwdc2005/

radmind

- Command line tools
  - Manages files on a hard disk
- Features
  - Free
  - Very popular
  - Open Source
  - Runs on many Unix platforms
  - SSL supported
  - Detailed configuration
    - Easy to specify what machine gets what
  - Detailed hard disk management
    - Every file is cataloged and stored on the server

radmind

- Unix command-line tools
  - Server daemon
    - `radmind`—talks to client tools
  - Client tools
    - `fsdiff`—finds changed files on a hard disk
    - `lapply`—undo's changed files
    - `lcreate`—uploads changed files to server
    - `ktcheck`—downloads file descriptions
    - More…

radmind

- `fsdiff`—How does it know what is changed?
  - The 1st scan becomes the “baseload”
    - It is uploaded to the server
  - All scans after that are the differences
    - Differences can be uploaded w/ `lcreate`
      - Called “overloads”
    - Differences can be undone w/ `lapply`
      - New files are deleted
      - Missing/modified files are replaced from server

radmind

- Simple example
  - Create 1st scan, the “baseload” (`fsdiff`)
  - Change something (Finder or other app)
  - Scan it again (`fsdiff`)
  - Remove the changes (`lapply`)
  - Or upload the changes (`lcreate`)

radmind

- Detailed example—Bringing a machine to the known state
  - Who knows what is on the computer
    - It doesn’t matter
  - Download descriptions from server (`ktcheck`)
    - Lists what files should be on hard disk
  - Scan hard drive and find differences (`fsdiff`)
    - Finds unknown and modified files
  - Undo differences (`lappy`)
    - Deletes unknown files
    - Deletes then re-downloads modified files
  - Machine is at known state

radmind

- Detailed example—Creating an overload
  - Machine is at known state (from previous step)
  - Install software
    - OS Update, Photoshop, Maya, Office, etc…
  - Scan for differences (`fsdiff`)
    - Finds unknown and modified files
  - Upload differences to server (`lcreate`)
    - Uploads unknown and modified files
  - Distribute those differences to other machines by editing configuration files on the server

radmind

- Each machine has a “command” file
  - Command file lists the overloads
    - 1st overload is the first scan, the baseload
      - Contains only the OS usually
    - Other overloads are apps or incremental changes
      - OS Update, Photoshop, Maya, Office, etc…
- All command files are stored on server
- Machines download the command file when running radmind (`ktcheck`)

radmind

- Configuring machines on server
  - Global config file
    - List machines and a command file
  - Machines can be specified by
    - Single IP
    - Range of IP's
    - DNS name
    - Symbolic name that matches an SSL Subject DN

radmind

- For more information about radmind
  - See www.radmind.org for links to
    - Manuals and Presentations
    - FAQ
    - Cookbooks
    - Mail lists
      - radmind-discussion
      - radmind-web
      - radmind-pc
- Contact radmind@umich.edu

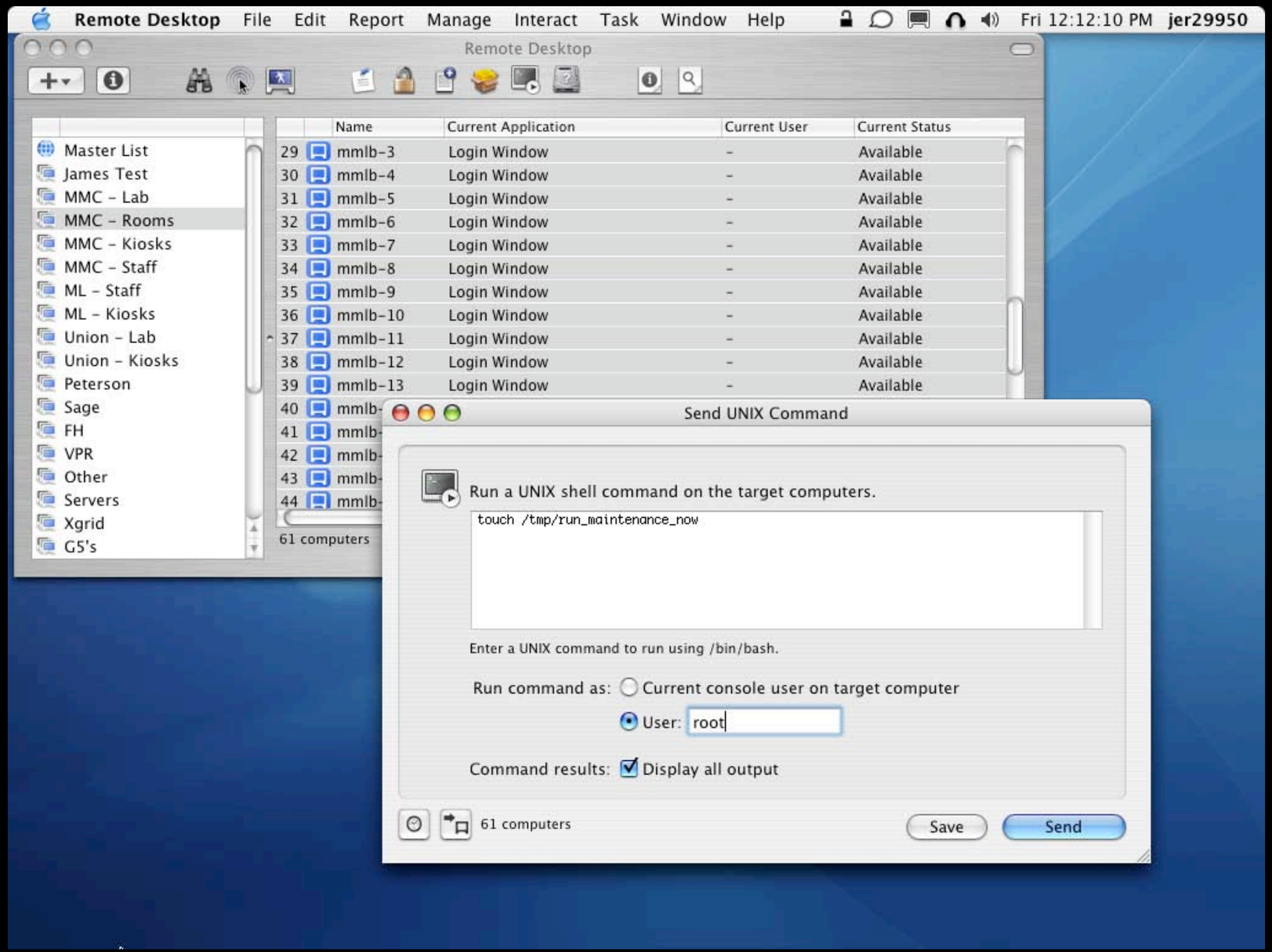
ULabMin

- Scripts, modifications, tools, graphics, and more
- Fills in the “missing links”
  - Automates the radmind tools (`fsdiff` and `lapply`)
  - Post-radmind tasks (what radmind can’t do)
  - Manages “cloned” home folders
  - Security audits
  - Manage printer settings
  - Manage resolution settings
  - Run a kiosk or other automated “drone”

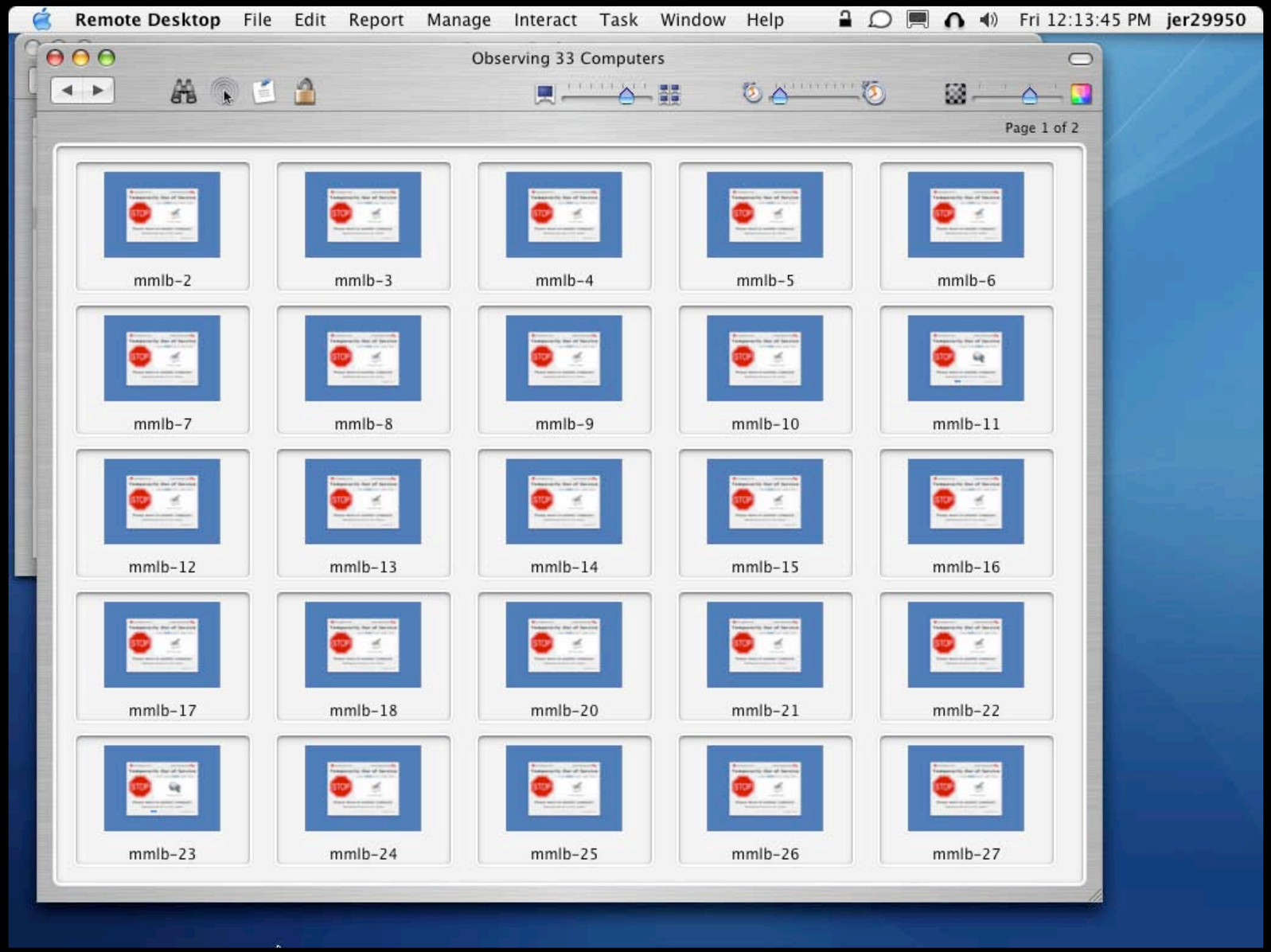
ULabMin

- Automates the radmind tools (`fsdiff` and `lapply`)
  - Uses iHook and scripts
  - Launch radmind easily
    - When logged in
    - When at the login panel
    - Remotely
    - At a specified time with `cron`
    - Ensure radmind finishes by running it at startup
      - (If users force restart the machine when it is running)

Automating radmind



How We Use radmind



How We Use radmind

ULabMin

- Post-radmind tasks (what radmind can’t do)
  - Updates prebinding
  - Sets preferences based on variables in a config file
  - Reports status of radmind runs to web db
  - Shows status in menubar and loginwindow

ULabMin

- Manages “cloned” home folders
  - Every user gets a “clean” home folder at login
    - Home folder is secure, private, and *works*
  - Lost and Found is maintained (and kept private)
  - Home folders are cached
    - Created when idle, swapped in at login

ULabMin

- Security audits
  - World writable files and folders reported to admin
  - Open Firmware password is checked
  - Webserver contacted (theft prevention)
- Manage printer settings
  - Users can add or delete printers
  - Defaults restored at each login
  - Requires no extra configuration from admin
- Manage resolution settings
  - Resolution set at startup and login

ULabMin

- Run a kiosk or other automated “drone”
  - Load a web brower instead of the Finder
  - Get rid of the Dock
  - Prevent Finder from running for kiosk user, but enabled for admin user
  - Make sure web browser window is always open
  - Cleanup the history and cache when screensaver activates

ULabMin—Lab Macs

ULabMin—Internet Kiosks

ULabMin—Reserve Desk

ULabMin—Presentation

ULabMin

- ULabMin is a super super hack and totally unsupported by Apple
- Tiger not supported yet, but will be in a few weeks…
- For more information about ULabMin
  - See www.macos.utah.edu/ulabmin
    - Documentation (still in progress)
    - Mail list
  - Contact ulabmin@scl.utah.edu

Q&A

Real World Desktop Management Practices

http://developer.apple.com/wwdc2005/

WWDC2005

Worldwide Developers Conference